Information Commissioner's Office: initial analysis of the European Commission's proposals for a revised data protection legislative framework

About this document

This document reflects the ICO's initial analysis of the European Commission's legislative proposals for the protection of individuals with regard to the processing of personal data. It is informed primarily by the ICO's extensive experience of regulating under the UK's current data protection law, which involves dealing with individuals' complaints, advising organisations and the public, and carrying out enforcement action.

This paper is not a comprehensive analysis of each element of the proposed Regulation or Directive, nor is it necessarily the ICO's last word on the subject. Our intention at this point is to provide an overview of the most significant parts of the proposed instruments and in particular to draw attention to those aspects which we believe still need further consideration. As the legislative process progresses, our analysis of some aspects of the proposed legislation is likely to become more comprehensive and detailed.

We hope our views will help to inform the debate and will be of use to all those – in the UK and beyond - with an interest in the successful implementation of next-generation European data protection law.

The Commission's proposals

The Commission's proposals are a positive contribution towards updating EU data protection law. We do not doubt that this is necessary. For example, e-citizens currently enjoy 'paper age' access rights, new ways in which individuals can be identified have come into being since current data protection law was conceived, and rules relating to international transfers no longer reflect reality.

Given the comprehensive updating that is needed, and the pan-European nature of the problem, we accept that either a Regulation or new Directive is needed. Simply updating the various national laws already in place could add to the lack of harmonisation that the European Commission wishes to address through its proposed Regulation. Doing nothing would mean that personal data will not be satisfactorily protected within the EU

and that businesses will continue to be expected to comply with a patchwork of out-of-date national laws that do not reflect current business reality.

As UK data protection law applies to all sectors, it would have been preferable for the Commission to have developed one comprehensive data protection instrument whether a Regulation or a Directive. Given the two different instruments proposed, it is important for there to be as much consistency as possible between these instruments. Furthermore, there are adverse implications for harmonisation by having one instrument which is a Regulation and one which is a Directive. However, a reasonably comprehensive and consistent framework can be achieved provided there is a common approach in both instruments as regards the 'core' aspects, such as principles, rights, obligations and supervision.

We are sceptical of the need for a two-year implementation period for both instruments. Data protection legislation is not a new area of law and many of the provisions are either already in force or recognised as good practice and given effect widely across the EU. We accept there may need to be a transitional period to implement some of the provisions, however, we would prefer implementation and compliance with the revised framework to be achieved more quickly once it enters into force.

Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General data protection Regulation)

Harmonisation

We understand the drive for harmonisation and, to the extent that this is consistent with effective data protection, we welcome the parts of the proposed Regulation that achieve this. We do though, make suggestions for improvement where we believe that a particular provision is unduly onerous or will not work well in practice. We have inevitably concentrated our attention on the areas of the Regulation where we feel improvement is most needed.

It should though be recognised that lack of harmonisation may partly result from a desire to accommodate 'external factors' such as different national legal systems, social norms or regulatory traditions. We have doubts as to whether complete harmonisation is possible, or even desirable, given that key concepts in the law such as fairness depend on these factors which necessarily vary from one member state to another. If taken too far, the drive for harmonisation will lead to burdens on business and complexity for individuals that may achieve harmonisation on paper but will not necessarily deliver sensible and effective data protection in

practice. The achievement of equivalent protection of personal data across the EU is probably more valuable for individuals than the harmonisation of rules.

Prescription and over-regulation

An obvious feature of the Regulation when compared to the current Directive (95/46/EC) is that it is far more detailed and prescriptive, particularly in respect of the measures it would require organisations to adopt to achieve and demonstrate compliance. A more prescriptive approach will not necessarily bring about better data protection. In any case, complete harmonisation is probably an unachievable goal.

There is a risk that the implementation of rules that may be perceived as onerous or disproportionate could actually lead to more variable standards of compliance by reluctant data controllers. For data protection to be effective in practice data controllers must be able to see a clear link between the measures they are required to take and the protection of privacy. Regardless of any penalties, if data protection is merely seen as legal 'red tape' or form-filling, it will not be effective in practice.

A somewhat more flexible instrument, with rather less emphasis on ensuring all data controllers follow common processes, and rather more on ensuring they actually deliver equivalent standards of privacy protection across the EU, might well bring about a better standard of data protection in practice. It should be possible to achieve this without sacrificing the key elements of the welcome and necessary enhancements of data protection that the Commission has included in its proposal.

Public access to official documents (Recital 18)

We welcome the recognition that the principle of access to official documents may be taken into account when applying the provisions of the Regulation, given that the UK has freedom of information law and as a member state we are subject to the Environmental Information Regulations. This should be reflected explicitly in the Articles, in particular in Article 6.

Despite the Recital, there could still be legal uncertainty where a public authority needs to process personal data to comply with a request for access - given the relatively tight 'lawfulness of processing' criteria set out in Art.6. This could be a particular problem where it is necessary to process 'special categories' of personal data to comply with an access request – the current derogations from the general prohibition on processing special categories of personal data provide no obvious basis for allowing this.

It should be put beyond doubt that it is lawful for a public authority to process personal data where this is necessary in order to comply with national or European access to official information law which, in any case, has to pay due regard to the protection of privacy.

Chapter I: General provisions

Personal or household activity (Article 2)

Art.2 provides an exemption from the Regulation for processing undertaken by a natural person without any gainful interest in the course of its own exclusively personal or household activity.

The question of whether individuals processing personal data – about themselves and others – particularly online – fall within 'personal activity' is an increasingly significant one for the ICO. The Regulation should not leave this in any doubt. It should be made clear that, in some contexts, processing online can still be in the course of a person's exclusively personal or household activity, for example, posting a blog about family matters.

We are pleased that the Regulation recognises the need to retain an exemption for exclusively personal processing. However, the reference to 'gainful interest' here might give the impression that only non-commercial activity can benefit from the exemption. It would be helpful to clarify that personal commercial activity – such as selling one's personal possessions on an auction site - can also fall within the exemption.

We can also envisage cases where an individual might process personal data with a connection to his or her professional or commercial activity, but should still benefit from the exemption. An example might be where a worker posts a blog detailing his or her day-to-day worklife experiences. There is a danger that narrowing this exemption unduly will infringe the individual's right to freedom of expression, for example for 'bloggers'.

We welcome the clarification that data controllers providing the means for domestic processing shall not themselves benefit from the exemption. However, this does not address the question of the extent to which organisations hosting personal data processed for domestic / personal purposes are responsible for that content. This is a particular problem where controllers do not exercise editorial control over content. The extent to which the responsibility of those providing online platforms for the publication of personal data is limited when they have little or no control of that data should not be left in doubt.

Territorial scope (Article 3)

We can see the advantage to EU data subjects of non-EU data controllers being required to comply with the Regulation, but we have considerable

doubt as to how far this is achievable in practice. While we can see the desirability of extending the territorial scope of EU regulation and recognise this should at least *encourage* non-EU organisations to adopt good practice and meet European standards for processing personal data – particularly when targeting services at EU citizens – in practice there may be little that European supervisory authorities and others can do in terms of enforcement unless effective cross border enforcement mechanisms can be provided. This means that, in reality, non-EU data controllers' compliance with the Regulation would be voluntary. The Regulation should be realistic about this and should not lead EU consumers to believe that the law offers them a degree of protection that, in reality, it cannot deliver.

It is also unclear how a supervisory authority could necessarily determine whether a particular company is offering goods or services to consumers in Europe, for example, would a company in the US that merely makes its goods or services available on a website which happens to be accessed by consumers in a member state be considered to be 'offering' its goods or services to them? Some clarification is needed.

Definitions (Article 4)

Data subject

We welcome the expanded definition of 'data subject'. It is particularly welcome that this definition makes it clear that an individual can be identified by an 'online identifier' as well as by 'traditional' identifiers. There is currently considerable uncertainty over the status of IP addresses, cookie identifiers and similar information generated online. The ICO's approach has been to advise organisations, as far as is possible, to treat this information as though it were personal data. Whilst this might work well in practice, it does not provide legal certainty for organisations or citizens.

We would prefer the Regulation to make it clear when these 'non-obvious identifiers' – as the ICO has referred to them – do constitute personal data, and when they do not. The formulation in Recital 24 – that such information need not necessarily be considered as personal data in all circumstances - does not really help. A better approach might be to make it clear in the Regulation that where IP addresses or similar identifiers are processed with the intention of targeting particular content at an individual, or otherwise treating one person differently from another, then the identifier will be personal data and, as far as is possible, the rules of data protection will apply.

Personal data

We also welcome the expanded definition of 'personal data' resulting from the expanded definition of 'data subject'. In combination, these definitions

make it clear that identification can take a number of forms and is not only based on 'traditional' identifiers such as names and addresses or reference numbers. However, the concept of identification can become increasingly problematic the further it extends beyond 'traditional' means of identification. We welcome the relative clarity that these definitions bring in terms of the scope of the Regulation. However, we are not sure why Recital 23 refers to 'means likely reasonably to be used' when Art.4(1) refers to 'means reasonably likely to be used'. The language of the Recital should be brought into line with that of the Article to ensure there can be no doubt about the intention behind the legislation.

Given the wide scope of 'personal data' we consider, based on our regulatory experience, particularly in the online world, that it may be unrealistic to expect all the requirements of the Regulation to apply fully to all forms of personal data that fall within its scope. We welcome the partial recognition of this in Art.10 but would like to see it more explicitly stated, perhaps in the recitals. This is particularly important in relation to pseudonymisation as there needs to be positive encouragement to data controllers to use pseudonymisation wherever possible.

Recital 26 of Directive 95/46/EC refers to the use of codes of conduct as a means for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible. The challenge of achieving effective anonymisation is an ever-growing one, which is reflected in the ICO's plans to produce its own code on the subject. It would therefore be both helpful and relevant to reproduce this reference in Recital 23 of the Regulation.

The data subject's consent

We are pleased that there is only one form of consent in the Regulation. The distinction between 'ordinary' consent and 'explicit consent' in the current law has caused a great deal of confusion.

We welcome the 'high standard' of consent provided for here. The issue of whether consent has or has not been given, and whether it can be implied by a particular action (or inaction), has long been a cause of difficulty for the ICO. Therefore we are pleased that it has been put beyond doubt that for consent to be valid, the individual has to do something to indicate consent. This means that data controllers seeking to rely on consent – which, depending on the circumstances, they may not necessarily have to do anyway – will have to put mechanisms in place to allow individuals to indicate their wishes. We welcome the recognition that 'any appropriate method' can be used to provide a method for indicating consent. In particular, context needs to be taken into account. For example, a patient who has given consent to treatment by a doctor should not need to give a

further specific consent to enable the doctor to keep a necessary record of that treatment.

We have reservations as to the invalidity of consent where there is a 'significant imbalance' between the data subject and the data controller. Whilst we can clearly see the purpose of this stipulation, it requires qualification. We accept that there is generally a significant imbalance between a worker and his or her employer. However, this does not mean that consent cannot be valid within an employment relationship. An example might be where an employer decides to ask employees for details of their next of kin in case there is an accident. The employee is not required to provide the information and will not suffer in any way if he or she fails to do so. In our opinion consent could be perfectly valid in a case like this, despite the general imbalance between employer and worker.

It is important that where consent cannot be valid – for example, because it cannot be freely given in a particular situation – alternative means of legitimising the processing can be found where the processing is otherwise necessary and legitimate or in the data subject's interests. The welcome strengthening of consent should not leave data controllers without a lawful basis for processing which is either necessary or unobjectionable.

Filing system

The question of whether or not information falls within a 'relevant filing system' has been a source of considerable contention in the UK since the Data Protection Act 1998 came into force. It has led to complicated arguments and court rulings about the structure of non-automated information systems, and to considerable uncertainty on the part of data controllers and individuals alike as to whether information is personal data or not. The definition in the proposed Regulation will do little to solve this problem. A better approach might be to focus on the accessibility of information relating to a particular individual rather than solely on the structure of system.

Main establishment

This definition assumes that the 'main decisions' as to purposes for processing and so on are all made in the same place. This will not necessarily be the case. Larger companies may well make their main decisions in different places, including in countries outside the EU. Equally if the focus is on where the processing takes place, it is likely that companies will undertake processing in several countries, or may even have outsourced it. The definition should reflect this.

Child

We do not see what purpose the definition of a child in Art.4(18) serves, given that the only substantive provision exclusively relevant to children is

that relating to consent which, in any case, uses a different age limit. This is in any case problematic given different ages of majority in member states and different approaches to concepts such as maturity and competence. These variations are reflected in Article 12 of the UN Convention on the Rights of the Child with which compatibility should be ensured.

We can appreciate why an age limit of 13 has been specified in Article 8. However, in our opinion, the Regulation should allow for children under 13 to access services without consent in some circumstances, for example, where a child wants to access a confidential support line or is taking part in an online activity that presents little or no privacy risk and is of such a nature that the child in question is capable of understanding the service's implications for him or her.

The logistical difficulties involved in obtaining verifiable parental consent should be borne in mind. In some cases a requirement for verifiable parental consent could lead to data controllers holding explicit personal identifiers about children and their parents where this would otherwise not be necessary, for example, where a child uses a service 'anonymously'. The ingenuity of children in circumventing age verification systems should not be underestimated.

Chapter II: Principles

Principles relating to personal data processing (Article 5)

We note that there is significant variation between the versions of the Principles that appear in the Regulation and in the Directive. Given the significance of the principles in forming the backbone of data protection law, we would like to see the two sets of principles harmonised. Otherwise, we fear there will be considerable confusion, particularly on the part of those data controllers who are required to comply with both the Regulation and the Directive in respect of their various data processing activities.

We welcome the references to data minimisation in principles (c) and (e). Although always implicit in the data protection principles' requirement of 'necessity', it is helpful to have an explicit reference to data minimisation in the principles. This is particularly significant as it supports the concepts of data protection by design and data protection impact assessments that also appear in the Regulation.

Both the Regulation and the Directive would benefit from provisions requiring the establishment of appropriate time limits for the retention and deletion of personal data and for a periodic review of these time limits.

Lawfulness of processing (Article 6)

We have always had doubts as to the approach taken in the Regulation – and in the current Directive – whereby there is a general prohibition on processing personal data unless a particular condition or 'gateway' exists. While this may work well in more strictly codified legal systems, it does not work particularly well in the UK, where the general rule, at least in the private sector, is that an activity can take place unless the law specifically prohibits it. However, we realise that the approach taken in the Regulation is a fundamental part of the European approach to data protection, despite the artificial prohibition on otherwise unobjectionable processing that it can create.

A particular problem might arise here in respect of the stipulation in Art.6(3) that the basis for processing in points c (legal obligation) and e (task carried out in the public interest / in the exercise of official authority) must be provided for in Union or member state law, particularly when coupled with the stipulation that point f (legitimate interests) cannot be relied on by public authorities. There is a danger that this will prevent public bodies carrying out processing that may well be necessary although not specifically provided for by law. It may also stand in the way of processing that is desirable, unobjectionable and helpful to citizens merely because the law does not specifically permit the public authority to undertake it. We would like to see an explicit recognition in the Regulation that processing may take place where it is clearly in the data subject's interests and does not override his or her fundamental rights and freedoms. This would help allow reasonable evolution in the delivery of public services that might otherwise be unhelpfully constrained.

Processing of special categories of personal data (Article 9)

We have previously expressed our doubts as to the value of the protection that categorising personal data into special (or sensitive) and non-special (or non-sensitive) categories offers to individuals in practice. In our view drawing a simple binary distinction between the two types of data fails to recognise the significance of context and the reality that one type of data might be sensitive for one person in one situation, but not for another or in different circumstances. We maintain our reservations about this approach.

As it stands we believe that there is a lack of correlation between the Regulation's list of special data categories and the sensitivities of citizens. From a UK perspective, we do not believe that trade-union membership is particularly sensitive but we do believe that most citizens would consider information about their financial status to be sensitive. Some data categorised as 'special' might not warrant special legal protection – for example a reference in an employment file to a worker's absence from work due to a common cold.

In any case we have more concern about moving from providing special protection for personal data revealing 'religion or philosophical beliefs' in Directive 95/46/EC to personal data revealing 'religion or beliefs' in the proposed Regulation. We have, for example, had a case in the UK where it was argued in an employment context that a belief in climate change was a belief worthy of protection. The use of the word 'beliefs' requires qualification. This might be achieved by instead using the formulation 'religion or similar beliefs'.

It is important that the presence of 'gaps' in the exceptions from the prohibition on processing special categories of data does not lead to a prohibition of otherwise unobjectionable processing. The Commission's power to adopt delegated acts should be used to take account of new developments, not to fill gaps that should be recognised and addressed on the face of the Regulation. One practical solution could be to introduce an additional condition for processing special categories of personal data where the processing manifestly does not impact adversely on the privacy of data subjects.

The wording of Art.9(2)(j) is ambiguous and in the UK has sometimes been read as meaning that the official authority is *required* to keep a complete register of criminal convictions. We assume that this is not the intention, and it would be helpful if the wording were amended to reflect this. This can be achieved by either substituting 'may' for 'shall' in the last sentence, or by rewording it to read 'where a complete register of criminal convictions is kept, it shall only be kept under the control of official authority'.

Processing not allowing identification (Article 10)

We presume that this provision is intended to deal with situations where organisations only hold 'non-obvious' identifiers about a person, for example an IP address linked to a particular device, and may then be faced with the problem of dealing with requests for subject access to the information. If so, this provision is welcome in that it will make it clear that organisations do not need to acquire the additional information – which they would not otherwise hold – to grant subject access or to comply with other parts of the Regulation.

Chapter III: Rights of the data subject

This is one of the parts of the Regulation that we most welcome, because we believe that it updates and strengthens' rights in a way that will be of particular benefit to individuals.

Transparent information and communication (Article 11)

We welcome the requirement for clarity, accessibility and plain language in policies relating to the processing of personal data. This very much

corresponds with the ICO's own approach, after noting that privacy policies, couched in difficult legal language, had often become exercises in corporate indemnification, rather than being genuinely informative to the public.

Procedures and mechanisms for exercising the rights of the data subject (Article 12)

We consider one month to be a reasonable period for dealing with a subject access request or an objection to data processing, particularly as the one month stipulation is a 'back-stop' period with data controllers being required to comply with requests 'without delay'. Being mindful of the large amount of personal data that is already available to data subjects in real time, for example, in an online bank account or electronic health record, we suggest that consideration be given to stipulating a shorter compliance time for requests made electronically for electronically held information. We recognise the greater expense and difficulty that can be involved in giving access to manually held data.

We assume that the extension of the compliance period to two months is intended to deal with situations where a large number of data subjects act in concert, all making subject access requests at the same time – perhaps even to deliberately inconvenience the data controller. We are aware of one or two cases where this has happened in the UK. If so, it would again be preferable to stipulate that the data controller must comply with the requests as soon as is practicable. If a very large number of requests are made it may be difficult to comply even within two months. However, as it stands, the wording here - 'several data subjects' – could involve a fairly small number of requests. We would expect these to be dealt with within the normal timescale. The extended timescale should only apply when the number of requests is both large and exceptional.

We do not believe that the current modest subject access fee arrangements in the UK create a problem for data subjects who genuinely want access to their personal information. However, the law should encourage data controllers to give direct, online access to personal data free of charge where this is feasible and no significant administrative costs are incurred by the data controller.

As the Regulation in Art.8(4) provides for requests which are manifestly excessive – or unreasonable – to be refused, there is no need to include provisions on charging a fee for these requests. It should be made clear whether the reference to 'in that case' in relation to the data controller bearing the burden of proof refers to the case of charging a fee or to the case of not taking the action requested, or both.

Rights in relation to recipients (Article 13)

We welcome this provision because in an information society where increasing amounts of information are shared and networked, inaccuracies should be corrected by all the data controllers holding the inaccurate data. We also value the provision in Art.14(3) that requires a third-party data controller to tell individuals where data about them originated.

Information to the data subject (Article 14)

We welcome the expanded 'fair processing' information that data controllers will be required to provide to the individuals they collect information about, particularly the requirement to inform individuals of their rights and their ability to lodge a complaint.

As it stands, the Regulation would always require the 'fair processing' information to be provided where information is collected directly from the data subject. We recognise the difficulty that could be involved in actively providing increasingly lengthy and complex 'fair processing' information in all cases. It should be made clear that it is acceptable for the 'fair processing' information to be readily accessible to the data subject, particularly where the processing is not contentious, unexpected or likely to have any detrimental effect on individuals, provided the existence of the information is flagged up. The derogations from the Regulation's fair processing requirements at Art.14(5) do not currently provide for this.

We support the obligation to inform individuals as to whether the provision of information is voluntary or obligatory, and interpret this as a clear link to data minimisation. However, we wonder whether 'obligatory' is meant to address cases where the individual is required by law to provide information, for example, in some official contexts, or whether the information is obligatory because it is actually necessary to provide the goods or services that the individual has requested, or whether it is obligatory simply because the data controller has decided that it should be. It should be made clear that information can only be labelled as obligatory where it is genuinely necessary for the individual to provide it.

It is not clear how data controllers should, in practice, inform individuals as to the level of protection afforded by third countries that the personal data may be transferred to.

While we can see how the Commission drafting standard 'fair processing' forms might help bring about harmonisation and perhaps help data controllers to comply with the law, the use of these forms should not be mandatory. It should be left open to data controllers to improve on any standard forms.

Right of access for the data subject (Article 15)

As with the 'fair processing' information in Art.14, we welcome the expanded set of information that must be provided to individuals making subject access requests set out in Art.15(1). However, data controllers should not be required to provide this information if it has already been provided as part of the process of obtaining the personal data.

It should be made clear that in online contexts, a data controller may make subject access information available to the data subject – for example through a secure portal – rather than by providing a copy of the data.

As with Art.14(8) above, the Commission providing standard forms for use when dealing with access requests could be useful. However, their use should not be mandatory.

Right to be forgotten and to erasure (Article 17)

This is one of the more interesting parts of the Regulation. Its implications for the information society need thinking through carefully – as does the challenge of making this right work in practice. On the one hand we can see the desirability of an individual being able to require the deletion or removal of information where there is no compelling reason for its retention. We can also appreciate that data controllers should able to justify their holding personal data about someone.

However, an insufficiently qualified right to be forgotten could have serious implications for freedom of expression - particularly the right to publish information - and for the maintenance of the historical record. An example might be where a public figure tries to use the right to remove embarrassing content from a newspaper archive. We recognise the derogations from the right to be forgotten provided for in Articles 80, 81 and 83. However, given these derogations, the various qualifications to the right and the technical difficulties surrounding online deletion, we are unclear how the right to be forgotten will be delivered in practice. There is a risk that if individuals are led to believe they have a 'right to be forgotten' they will be disillusioned if they find that the right is strictly limited in practice. It might be preferable if this right was presented in less ambitious terms.

We do think that individuals who choose to post information about themselves – typically on a social networking site – should generally be able to secure its removal easily. We would welcome this being made a legal requirement – albeit that once cached and published elsewhere it may be impossible to remove the information entirely from the internet. We also believe that where a third party publishes information about an individual, the publishing should cease in certain circumstances – however

this seems to be provided for adequately in the Art.19 right to object to processing. It would also seem that in some circumstances the application of the data protection principles and the Regulation's data minimisation requirements would require deletion anyway – for example where the publication of personal data is no longer necessary.

The words from 'especially' onwards should be removed from the first paragraph of this Article. Although there can be explicit exemptions, individual rights are either applicable or they are not. It does not make sense to say that rights are 'especially' applicable in some cases. Using this formulation creates unnecessary uncertainty and calls into doubt whether individuals actually have a 'right to be forgotten' in relation to personal data other than that made available when they were a child.

We do not understand the reasoning behind the reference to 'authorised' in paragraph 2. We are not sure in what circumstances a data controller will authorise a third party to publish its content. A more likely scenario would be where the third party 'harvests' and republishes content on its own website, quite possibly without the knowledge or consent of the original data controller. This is perhaps an example of why the right to be forgotten might be difficult to achieve in practice.

Right to data portability (Article 18)

We support the idea of individuals having a right that will help them to transfer their personal data from one service provider to another. We can see benefits for the individual in this, from both a consumer protection and a competition perspective.

There is a danger that data controllers will seek to circumvent this provision by holding information in non-standard formats. The right might be more effective if it were to require data controllers holding information in a non-standard format to convert it into a standard one, where this is reasonably practicable, should an individual wish to exercise his or her data portability right. We recognise this might present a burden on data controllers, and that it could be argued that the ability to easily change providers is more of a consumer issue than a data protection one. However, it would help ensure a level playing field given that initiatives in some member states (such as MiData in the UK) are encouraging companies to develop services or to hold data in formats which allow data subjects to use personal data for the data subject's own purposes.

There should be provisions that allow data controllers to protect their trade secrets and intellectual property rights when complying with the data portability right.

Right to object (Article 19)

There is a significant shift here from the current situation – where the individual only has a right to prevent processing where he or she can demonstrate that unwarranted damage / distress is being caused. The provision in the Regulation would mean that the default position is that the individual has a right to object, and the data controller has to demonstrate why the objection is invalid. We welcome this because it gives individuals a greater degree of control over information about themselves by changing the burden of proof, meaning that data controllers have to be able to justify their processing of personal data. However, it is important that a data controller will be able to refuse an objection where there are compelling legitimate grounds for continuing to process the personal data. Our experience suggests that individuals can sometimes expect cessation of processing in unrealistic circumstances – for example where an individual wants his or her credit reference file deleted but still expects to have a credit application accepted. The 'compelling legitimate grounds' exception will presumably address situations like this.

Measures based on profiling (Article 20)

It is not obvious whether profiling carried out to deliver content to an individual, for example, through behavioural advertising, falls within the scope of this Article. Recital 21 refers to profiling to deliver online content. However our view is that it does not, given that it would be difficult to argue that the type of activity described in Recital 21 produces legal effects or significantly affects data subjects. This does though need to be put beyond doubt.

This Article lists a number of different 'personal aspects' with very varying degrees of impact on individuals' privacy. For example, the analysis of a person's performance at work could have far greater consequences for the individual than the delivery of online content based on analysis of online behaviour. A more risk-based approach – perhaps linked to a data controller carrying out a data protection impact assessment – could provide more effective safeguards for individuals. We do though welcome the additional level of control and protection that this Article is intended to provide to individuals.

Restrictions (Article 21)

The restrictions on the obligations and rights provided for here should also extend to the prevention, investigation, detection and prosecution of data protection breaches and to monitoring, inspection or regulatory functions connected with these, that is to the work of data protection supervisory authorities.

Chapter IV: Controller and processor

Responsibility of the controller (Article 22)

We certainly agree that data controllers that process personal data should be able to demonstrate their ability to comply with the law by having the necessary policies, administrative measures and personnel in place. This is the essence of accountability. A failure to be able to do this should certainly be an aggravating factor should enforcement action be considered against a data controller. However, we would find it problematic to take action against a data controller for not having the necessary 'paperwork' in place where the processing carried out by that controller would be otherwise fair and lawful and has not had any detrimental impact on individuals' privacy. That would seem unfair and disproportionate from a regulatory perspective. Rather than mandating in detail how the measures set out in Art.22(2) are to be achieved, a better approach might be to promote these measures as good practice. The law could make it clear that a data controller must be able to demonstrate that it has taken steps to ensure compliance, including measures such as these. Any failure to do so would be taken into account in the event of enforcement action in respect of a failure to comply with the substantive requirements of the law, for example, where a security breach has occurred.

We note that Art.22(4) allows room for specific measures in respect of micro, small and medium-sized businesses. We presume this is intended to enable the Commission to introduce further measures to ensure that the responsibilities on the controller are proportionate to the nature of the controller's business. This is important as many smaller businesses carry out routine, low-risk processing about their staff and clients and should not necessarily be required to have the same comprehensive data protection compliance mechanisms in place that are likely to be needed for larger businesses. (This could of course also be the case with some larger organisations undertaking low-risk processing.) We would welcome a clearer indication of the Commission's intentions in relation to measures for micro, small and medium-sized businesses.

Data protection by design and by default (Article 23)

The ICO has a long history of promoting privacy by design and privacy by default approaches, and we are pleased to see these recognised on the face of the Regulation. However, it is important that they are applied in a way that is proportionate to the risks posed by the processing of personal data by, and the resources available to, individual businesses and in particular to small and medium-sized businesses.

Representatives of controllers not established in the Union (Article 25)

The reasoning behind the exceptions from the requirement to designate a representative in Art.25(2) is unclear. For example, a controller established in a third country with an adequate level of protection could breach the requirements of the Regulation without necessarily breaching the law of the third country in which it is located. The need to designate a representative in the EU which can be addressed by supervisory authorities and data subjects still remains. These exceptions either need to be removed or justified.

Documentation (Article 28)

We have no doubt that effective data protection requires data controllers and processors to maintain appropriate documentation. We are not though convinced that it is either necessary or helpful to prescribe in detail the extensive range of documentation set out in Art.28(2). This not only replicates the documentation required under the notification provisions of the current Directive, but adds to it, thereby increasing rather than decreasing the burden on data controllers and processors in a way that does not seem to be proportionate to any privacy gains. Again there is too much emphasis on mandating the bureaucracy of data protection when the objective of the Regulation is the protection of personal data in practice rather than the creation of paperwork. We would favour a formulation that concentrates more on the desired outcome, along the lines of requiring data controllers and processors 'to maintain such documentation relating to the nature of the personal data held, its sources, its processing and its disclosure as is necessary to enable the controller or processor to meet its responsibilities under this Regulation for the protection of personal data'. It is not necessary for the achievement of high data protection standards that all controllers and processors maintain precisely the same documentation.

Notification of personal data breaches (Article 31)

We are strongly in favour of a legal requirement for data controllers to notify data breaches in certain circumstances. However, it is important that the law puts proportionate breach notification 'triggers' in place. Otherwise, there is danger that supervisory authorities will be swamped with notifications of trivial or inconsequential breaches. Although the Commission has suggested that there will be a 'trigger', there is nothing on the face of the Regulation that guarantees this.

We can understand the need to require data controllers to notify breaches promptly, but a target of 24 hours appears unrealistic. In any event, as the Article stands, it would be open to data controllers to argue that it was not 'feasible' to comply within 24 hours. However, this involves providing a 'reasoned justification' to the supervisory authority. If, in practice, few if

any breaches can be notified within the 24-hour period, then data controllers will be faced with unnecessary administrative burdens of providing a justification when they should be focusing on dealing with the breach. A simple requirement for notification 'without undue delay' would be preferable. This is, after all, the wording used in the revised e-Privacy Directive (2009/136/EC) and using it in the Regulation would ensure a degree of consistency.

We welcome the provision in Art.32 for individuals themselves to be notified of a breach. However, the duty to notify individuals should not be linked solely to the effect of the breach on the protection of personal data or privacy. Financial loss, embarrassment or other negative effects should also form part of the 'trigger' mechanism for notifying individuals.

We do not see why the supervisory authority should be notified before the individual. In some cases the duty on the data controller should be to notify the individual at the same time as the supervisory authority or arguably before. We note that the relevant Articles do not specify any timescale for a supervisory authority to act on a breach notification. This means that there is a danger that the notification will sit in a backlog at the supervisory authority whilst the individual remains unaware of the breach and is vulnerable to financial loss, for example, where banking details have been lost. In some cases earlier notification to the data subject would be necessary to allow the data subject to take steps to reduce their vulnerability.

Article 32(3) refers to technological protection measures that render data unintelligible to any person who is not authorised to access it. We have doubts as to whether this provision is consistent with the technological neutrality of the Regulation. In any case we are not convinced that the loss or disclosure of information that is rendered inaccessible constitutes a personal data breach. Furthermore, the Regulation should make it clear that the need to demonstrate technological protection measures to the supervisory authority shall be at the request of the authority, not in every case.

Data protection impact assessment (DPIA) (Article 33)

Again, the ICO has been a long-standing supporter of 'privacy impact assessments', which seem to be substantively the same as the DPIAs provided for in this Article.

We are pleased that DPIAs are being mandated for data controllers whose processing presents specific risks to the rights and freedoms of data subjects. We are content that the risk criteria set out in Art.33(2) mean that DPIAs will be only required when data controllers are carrying out large-scale and / or sensitive data collection.

We would favour an additional provision requiring data controllers to publish summaries of DPIAs, subject to appropriate exemptions to protect security and commercial confidentiality. The case for this is particularly strong where the data controller is a public authority.

Prior authorisation and prior consultation (Article 34)

The purpose of this Article is confused, as it appears to conflate prior authorisation for domestic processing with prior authorisation for the overseas transfer of personal data. It would be helpful if the provisions relating to overseas transfers were moved to Chapter V.
However, as we understand it, this Article is intended to give supervisory authorities the opportunity to vet certain data processing activities, particularly involving the overseas transfer of personal data, before they take place, so that they can be authorised or prohibited.

These provisions need to be examined against a backdrop of an enormous and growing volume of international online data transfers, where data about millions of people can be processed anywhere at any time. It is worth noting that we have not been presented with any evidence to suggest that international transfers from the UK, where there is currently no prior authorisation mechanism, have resulted in data subjects being disadvantaged or personal data being misused. We believe that the provisions here that require prior authorisation are disproportionately burdensome and bureaucratic – for both data controllers and supervisory authorities.

Our own preferred approach to the Regulation of overseas transfers would be to start by ensuring that data exporters know that they are responsible for identifying and minimising risk and are aware of their liabilities under the law. We then think it important that data controllers enjoy flexibility as to how 'adequacy' can be ensured. It is highly unrealistic, and perhaps undesirable, for supervisory authorities to be expected to routinely authorise, or prohibit, large volumes of data transfers. The decisions are properly ones for data controllers who must be encouraged to assess risk, to make their own decisions about data processing, to be accountable for these decisions and to face enforcement if they get it wrong. Given that the proposed Regulation places a great deal of emphasis on data controllers taking their own responsibility for their processing activities, it seems somewhat contradictory to give the supervisory authority a direct role in managing this aspect of compliance.

Data protection officers (Article 35)

We can certainly see the desirability of organisations that are involved in large-scale data processing, or that are involved in 'risky' processing, having a member of staff that is responsible for oversight of data protection compliance. However, we do not believe that data protection officers, of the form envisaged in the proposed Regulation, need

necessarily be mandatory, provided that organisations have effective processes in place for ensuring data protection compliance. We would prefer the appointment of data protection officers to be encouraged as good practice, with failure to have someone with clear data protection responsibility being citeable as an aggravating factor where a supervisory authority considers enforcement action. This would also take account of the different ways organisations operate, as responsibility for data protection compliance does not always fall to one specific individual.

We do not in any case believe that the appointment of a data protection officer should be linked to the number of employees in an enterprise. There are businesses with a large number of employees that only engage in relatively low-risk processing, for example, the routine maintenance of records about their staff and customers. On the other hand there are online businesses that process a great deal of varied information about people from all over the world but which have relatively few employees. A better approach might be to assess any requirement to have a data protection officer according to the number of data subjects the organisation processes data about and / or the nature of the data concerned.

We certainly agree that if a data protection officer is appointed, he or she should have the necessary knowledge and experience to do the job effectively. However, a data controller that appoints someone as data protection officer who lacks the required professional qualities could presumably fall foul of Art.79(6)(j) and be liable for a fine of up to 1,000,000 Euros. Does this mean that supervisory authorities would be expected to check the knowledge, ability and so on of the officer in question? This could be difficult to do in practice.

The approach to independence taken in Art.36(2) needs further consideration. We accept the importance of functional independence if the data protection officer is to have the sort of internal supervisory role envisaged by the Commission. However, this is not the only possible approach nor necessarily the best. It has not, after all, been adopted widely even within the EU. Even with this approach proper recognition still needs to be given to the fact that the data protection officer will remain an employee of the data controller and will generally be subject to its normal corporate standards and procedures. However, other approaches should not be ruled out. The idea of having a 'Chief Privacy Officer' who is a senior executive with an ability to influence decision making at the highest level but who also needs to be part of senior management not 'independent' from them has much to commend it. We believe this approach is more likely to drive sustainable long-term privacy improvements than a data protection officer whose role is more procedural in nature.

Codes of conduct and certification (Articles 38/39)

We welcome the duty on supervisory authorities to encourage the drawing up of codes of conduct. Our experience of regulating under the current data protection law confirms that data controllers must themselves play a major part in establishing data protection standards and compliance mechanisms. We are strongly supportive of the development of data protection seals and marks – particularly insofar as this will encourage consumers to transact with companies that offer high standards of privacy protection.

Chapter V: Transfer of personal data to third countries or international organisations

General principles for transfers (Articles 40-43)

The ICO has in the past called for a radical rethink of the way transfers of personal data overseas are treated under data protection law. Given the sheer scale of international transfers, we have significant doubts as to how meaningful any attempt by supervisory authorities to closely monitor, control or authorise transfers can be. Our own favoured approach would be to ensure that data exporters are aware of their responsibilities – wherever the processing takes place – and have the tools necessary to assess risk and to ensure compliance. Failure to do so would, as with a failure to meet the other requirements of this Regulation, leave the data controller open to enforcement action by supervisory authorities and claims from individuals.

We would therefore prefer the Regulation to take an approach to international transfers that is very much based on data exporters assessing risk and putting their own arrangements in place for making sure that when they do transfer personal data overseas it continues to be protected to an adequate standard. The provisions in the current Directive that set out the factors to be taken into account in assessing adequacy could helpfully be reintroduced here.

We recognise the value of binding corporate rules as a means of ensuring adequacy. However, we do not believe that supervisory authorities need to have a role in authorising or approving binding corporate rules – they should, though, be required to offer guidance and assistance to those drawing up BCRs or using other means to legitimise overseas transfers of personal data. Of course the presence of a properly drafted set of BCRs should be taken into account as a mitigating factor should a supervisory authority contemplate enforcement action against a data exporter.

We do not understand why the derogation in Art.44(1)(h) is restricted to data transfers that are not 'frequent or massive' These terms are not, in any case, defined and could be open to different interpretations. In our

opinion 'ordinary', routine transfers should be able to benefit from the derogation where the transfer is in the data controller's legitimate interests and where the necessary safeguards have been put in place, in other words where there is adequate protection. This would be a less burdensome approach to transfers and would not, in reality, undermine the protection afforded to data subjects. However, it would be misleading for this to be classed as a derogation. The data exporter's assessment of adequacy should be recognised as a proper ground for transferring data by way of appropriate safeguards under Article 42.

Chapter VI: Independent supervisory authority

Independence (Article 47)

We welcome the explicit requirement that data protection supervisory authorities shall be completely independent and properly resourced. We also consider that, for the sake of consistency, it is desirable that in member states the same authority should supervise compliance with both the Regulation and the Directive.

We are though concerned about the totality of the duties placed on supervisory authorities by the Regulation. This will have considerable resource implications which need to be thought through by member states. We wonder if member states are truly committed to providing the funding necessary for supervisory authorities to properly undertake all the duties imposed on them by the Regulation. The duties incumbent on supervisory authorities must correspond with the resources available to them. Otherwise there is a risk that the public will be led to believe that they enjoy a level of protection that, in reality, their supervisory authority cannot deliver. Supervisory authorities may also become a barrier to businesses if they are unable to perform all of the actions required of them, and in particular any prior approval or response to mandatory consultations, within reasonable timescales. Unless there is a genuine commitment to significantly increased funding the duties on supervisory authorities will need to be selectively scaled back to those which give the greatest value for money in terms of the protection of personal information.

Competence (Article 51)

We understand what this Article is trying to achieve and are supportive of the idea that there should be a 'one stop shop' or lead supervisory authority for businesses operating in a multiplicity of EU member states. This should ensure consistent application of the law which will benefit both individuals and businesses. However we are concerned as to how some aspects of the Article will work in practice.

The provisions in 51(2) link to the definition of 'main establishment' and the difficulties of this definition, as mentioned previously, mean that it will

be not always be easy to ascertain which is the competent supervisory authority for organisations operating in more than one member state.

If the main establishment is simply where the decision making takes place this will not properly address organisations which have decentralised decision making or which have decision making for different aspects of their processing located in different countries. This could lead to either several supervisory authorities assuming competence, or none at all particularly as it is not immediately clear whether the competence of the supervisory authority referred to in Article 51(2) is exclusive or shared.

If no decisions are taken in the EU and the main establishment is where the database or processing is located, this would not address organisations with databases in several countries, or those which may be established in the EU but which outsource their processing to a third country. This could again lead to either several supervisory authorities assuming competence, or none at all.

Furthermore, it is not clear how, if at all, this provision will apply to businesses which, as is often the case, have a high degree of centralised control but operate as separate legal entities, and so are separate data controllers in each member state where they have a presence.

We suggest concentrating less on identifying the 'main establishment' and more on having several criteria to narrow down which should be the lead supervisory authority. In any event the competence of the lead authority should not be exclusive. The lead supervisory authority would need to co-operate with and request assistance from other involved authorities. Criteria for selection of the lead authority could include the following.

- Where the organisation's HQ is located. If outside the EU, is there an EU HQ or main office?
- Where the decisions are made relating to the processing in question.
- Whether the organisation has an individual (like a Chief Privacy Officer or high-level data protection officer) or team in place to deal with supervisory authorities on behalf of the company and, if so where they are located.
- Where the actual processing in question takes place.
- In which member states affected individuals are located.
- In which member states individuals who have complained to a supervisory authority are located.

This could lead to the conclusion that the supervisory authority in a particular member state is best placed to take the lead. If the above criteria lead to the possibility of several supervisory authorities in different member states taking the lead they could agree among themselves which should take on this responsibility. If agreement cannot be reached, the EDPB could decide which should take the lead based on the above criteria.

It is in any case likely that a case-by-case approach is needed, which might not necessarily deliver a complete one-stop shop, in the sense that company A always deals with supervisory authority X for all data protection matters. This might not be realistic in terms of how companies are set up and operate. It is also worth bearing in mind that the majority of organisations in a member state are specific to that member state and the determination of the competent authority will be straightforward in most cases. It is only in a relatively small number of cases where organisations operate across several member states, and there is an issue that requires supervisory authority involvement, that the need to determine a lead competent authority will come into focus.

Duties (Article 52)

We are generally content with the Article dealing with the duties of supervisory authorities subject to the comment above on resource implications. However, we would like further thought to be given to complaint handling. We take the view that supervisory authorities should be able to be selective, pursuing only those complaints that reveal genuine privacy risks. To an extent Article 52 allows for this. However our experience suggests that complainants are often seeking resolution of an individual problem or some form of individual redress – for example, they may want to be compensated because their record is inaccurate. We would like to see an element of resolution, practical assistance to the public and redress for individuals reflected on the face of the law, including the availability of alternative dispute resolution mechanisms - even if this is not a function of the supervisory authority itself. (Art.75 partly addresses this, but only through recourse to the courts.)

Chapter VII: Co-operation and consistency

Consistency mechanism (Articles 57/58)

Given the scale of international online business, we have reservations about the practicality of supervisory authorities being required to inform the European Data Protection Board whenever they apply a measure that relates to processing activities which are related to the offering of goods or services to data subjects in several member states, or to the monitoring of their behaviour. In reality, this could mean that a supervisory authority would have to inform the EDPB whenever it takes any action against a company that operates internationally. This would be burdensome and, through the delay inevitably involved, could impact on protection for individuals.

It is not entirely clear what would happen if, for example, the UK supervisory authority were to approve a set of binding corporate rules but, once informed of the approval, the EDPB takes issue with it. We assume

that the supervisory authority's approval would still be valid, which begs the question of the nature of the EDPB's role here.

The EDPB could clearly exercise a great deal of power under the new Regulation. It is our assumption that the arrangements in the Regulation that relate to the appointment, conduct and so on of members of the national supervisory authorities will apply to the chair of the EDPB. If this is wrong comparable provisions are needed. It is not clear why one of the vice-chairs of the EDPB should be the European Data Protection Supervisor, as provided for in Art.69. We do agree though that it is a sensible, practical measure for the EDPS to provide the secretariat for the EDPB.

Given the considerable power vested in the EDPB we would also like to see the Regulation specify certain other aspects of its governance. Whilst the Regulation addresses confidentiality, it does not address transparency. We would like to see a requirement for the EDPB to consult with the relevant parties, or members of the public, when it adopts an administrative measure. We are aware of the criticism that has been levelled at the current Art.29 Working Party in respect of its lack of transparency and failure to engage with data controllers and the public. New data protection law provides an opportunity to remedy this.

We consider that it is going too far for any supervisory authority or the EDPB to be able to request that *any* matter be dealt with through the consistency mechanism, as provided for in Art 58(3). The consistency mechanism should be limited to issues of particular significance for data controllers or data subjects that have impact in several member states.

The Commission should be able to provide its legal opinion, but in principle must refrain from interference in the decisions of the EDPB made under the consistency mechanism. A procedure could be envisaged whereby, if serious problems arise, the Commission or the EDPB can ask the European Court of Justice for an opinion. For example, if the EDPB cannot agree on the application of the Regulation in a particular matter, it should be possible to ask the ECJ for a ruling. It is important to bear in mind that although the Commission has its own form of 'independence' this 'independence' does not qualify it to exercise independent data protection supervision.

The timescale set out in Art.58 is unrealistic and need to be revisited.

Suspension of a draft measure (Article 60)

It follows that the power in Art.60 to suspend a supervisory authority's draft measure should not be in the hands of the Commission, otherwise the principle of independent data protection supervision will be undermined. On matters that are properly referred to it, the EDPB should

have a mechanism for reaching a decision that is then binding on individual supervisory authorities. If necessary any decision could be challenged at the ECJ. Any interim measure, such as a 'warning' to a supervisory authority, would be addressed in the EDPB's rules of procedure.

Implementing acts (Article 62)

At many points in the Regulation there is provision for delegated acts to be brought into force. We understand that there are practical and legal reasons for this, but the provision for so many delegated acts does, in some places, leave considerable uncertainty as to the practical consequences of the Regulation. Where possible, we would like to see relevant provisions on the face of the Regulation itself.

We would also welcome an indication from the Commission as to whether it is their intention to implement these Acts, or some of them, at the time when the Regulation comes into force, whether they are to be held in reserve – for example to deal with future technological challenges to privacy. It would be helpful if the Commission could provide a schedule of all the opportunities for delegated and implementing acts and their intentions in respect of each of these.

We would also like to see a commitment to consult with the EDPB and national supervisory authorities, where appropriate, before delegated Acts are brought into force. This would reflect the position in the UK where the Information Commissioner generally has to be consulted before the Government introduces delegated legislation under the Data Protection Act 1998.

Enforcement (Article 63)

The full implications of an enforceable measure of the supervisory authority of one member state being enforceable in all member states concerned needs to be thought through. It is not clear to us just what is meant by an 'enforceable measure', how this will be made to work in practice or how well it corresponds with European legal convention where, as we understand it, only the rulings of the highest courts are binding on member states.

Chapter VIII: Remedies, liability and sanctions

Right to lodge a complaint with a supervisory authority (Article 73)

We support the idea of a 'one-stop shop' for data subjects. However, as it stands, Art.73(1) could mean that any data subject anywhere could complain to any supervisory authority about any data controller. This might mean that a Finnish data subject who has a problem with a Swedish

data controller could complain to the Irish supervisory authority, presumably in his or her own language, because he or she believes that the Irish will provide a better standard of service and a more advantageous outcome. This could provide considerable practical problems and logistical difficulties as well as being resource intensive. Perhaps a qualification relating to the submission of a complaint in the data subject's place of habitual residence or the place of establishment of the data controller would be appropriate.

Right to a judicial remedy against a supervisory authority (Article 74)

We do not think that one supervisory authority should be able to initiate proceedings against another authority. Where there is a dispute of this sort, EDPB should bring about a resolution with the possibility of a reference to the ECJ. This provision runs counter to the principles of and provisions for co-operation and mutual assistance.

Right to compensation and liability (Article 77)

The term 'damage' is interpreted in UK law as meaning only a loss that is material and quantifiable. It is though clear that the Commission's intention is to provide a right to compensation for psychological harm or even just embarrassment. We agree that this is the right approach and suggest it is put beyond doubt by referring here to compensation for the 'damage or distress' suffered.

Administrative sanctions (Article 79)

For the various types of violation, the supervisory authority is required to impose a fine of 'up to' a particular amount. Whilst this could mean quite a modest fine we take the maxima in the Regulation as being more indicative of the level of fine that could and perhaps would be expected to be imposed. If this is the case, then the nature of the violations in the various categories needs further thought. Indeed we have doubts whether specifying in such detail all the possible breaches and the level of fine that follows is either helpful or proportionate. We do not believe it is right, for example, for a data controller to be liable for a fine of up to one million Euros simply for failing to carry out a data protection impact assessment without there being any evidence that failure to do this has necessarily impacted on the privacy of individuals. (We do recognise, though, that a failure to carry out a DPIA, or to appoint a Data Protection Officer, for example, could, in some circumstances, have wider privacy consequences than a data controller's failure to deal properly with an individual's subject access request and that this may account for the relatively high tariffs for certain administrative failures.)

What is missing in the Commission's proposal is a link between administrative failure and practical consequence. Fines should not be

imposed for procedural or record keeping failures alone. The purpose of the Regulation is to protect the privacy of personal information and proportionality requires there to be a demonstrable link between any fine and a failure by an enterprise to achieve this. Fines should only be imposed for procedural or record keeping breaches of the Regulation where it is possible to demonstrate a clear link between the breach in question and the creation of a significant risk to privacy. Furthermore, the possibility of disproportionately high penalties for a failure to report a data breach to the supervisory authority or a failure to consult the supervisory authority when carrying out risky processing will drive over-reporting. This will place unnecessary burdens on supervisory authorities and divert them from addressing areas of genuine and significant risk.

We do not favour the 'shall impose' formulation in this Article. We would prefer 'may', as this would allow regulatory discretion and facilitate supervisory authorities' compliance with Better Regulation Principles. Indeed it is hard to see why supervisory authorities should be given discretion to apply a fine as low as one Euro with all the administrative effort this would involve, but not discretion to apply no penalty at all. We also very much doubt whether any supervisory authority would have the resources necessary to deal with the administrative burden of imposing a fine for each and every technical breach of the legislation.

The link between level of fine and company turnover is problematic, because it will hit high turnover but small profit organisations harder than ones with a relatively low turnover but a high profit margin. There are also practical difficulties for supervisory authorities in determining the relevant turnover of an enterprise, particularly when, as may be the case, the enterprise is a public authority or is a private rather than a public company.

It is very important that the activities of unlawful disclosure of personal data and unlawful obtaining of personal data (commonly known as 'blagging') that are currently addressed in Section 55 of the Data Protection Act 1998 can continue to be treated as breaches of data protection law in the UK and attract criminal sanction after the Regulation comes into force. These are offences that are very often committed by individuals rather than legal persons and a criminal sanction is much more effective than a civil penalty, both as a sanction and as a deterrent. We understand that this is likely to be the case but would welcome the matter being put beyond doubt.

Chapter IX: Provisions relating to specific data processing situations

Employment (Article 82)

Our experience suggests that the processing of personal data in the context of employment is a highly significant area – both for individuals and for data controllers. We are unclear as to the origins or the special treatment of processing in this context but can see why member states might see the need to adopt specific rules. However, it is important that such rules do no more than particularise and complement the provisions of the Regulation so that it still applies fully in the employment context.

Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

It is welcome that the Commission have proposed legislation that attempts to cover police and law enforcement sector processing of personal data both at national level and for cross-border exchanges. In doing so the proposed Directive will repeal the data protection framework Decision 2008/977/JHA, which did not include national processing in its scope. However, given the UK's protocol in the area of freedom, security and justice measures, it remains to be seen whether the UK Government will implement the proposed Directive to include national-level processing of personal data.

The proposed Directive includes some provisions which are the same or similar to those in the proposed general data protection Regulation, and comments made on those provisions above will not be repeated here.

It is our view that many provisions in the proposal have been considerably weakened when compared to the version made available online in December 2011 and when compared to the proposed Regulation. Many of our comments reflect this fact and call for certain wording or provisions to be reinstated to strengthen the level of data protection. This is particularly important in the police and law enforcement sector where the processing of personal data carries significant risk for individuals. At the very least the basic provisions such as the definitions and the principles related to data processing need to be aligned. A failure to do so runs contrary to the Commission's desire for consistency, is difficult to understand and explain and will only lead to confusion for data subjects and data controllers alike.

Chapter I: General provisions

Subject matter and objectives (Article 1)

The wording of Article 1(2)(b) suggests that an aim of the Directive is the freeflow of data, in a similar way that it is an aim under the Regulation. However, the processing covered by the Directive is not subject to the

same internal market. The wording should be clear that the aim is in fact that the principle of availability should not be unduly restricted for data protection reasons.

Definitions (Article 3)

The definitions are consistent with the Regulation. However, despite the inclusion of a definition of genetic data, a separate recital and Article on the handling of this kind of data has been removed as compared to the December 2011 version. This provided an important safeguard in relation to the use of genetic data and its retention periods. This is particularly important given the decision of the European Court of Human Rights in the Marper case relating to the retention of DNA.

It is not entirely clear what the difference is between a 'controller' (Article 3(6)) and a 'competent authority' (Article 3(14)).

Chapter II: Principles

Principles relating to personal data processing (Article 4)

As previously stated, we would expect the principles to be consistent across both instruments. However, this is not the case and the recitals of the Directive fail to include important elements regarding the retention of personal data, transparency towards individuals, keeping personal data up to date, and ensuring it is adequate, relevant and not excessive. Accountability provisions requiring the data controller to demonstrate compliance are also missing.

The December 2011 version also included provisions limiting access to data to duly authorised staff in competent authorities who need them for the performance of their tasks. This should be reintroduced.

Distinction between different categories of data subjects and different degrees of accuracy and reliability of personal data (Articles 5/6)

It is welcome that competent authorities are required to distinguish between categories of individuals, however, guarantees regarding those not convicted or where there are no serious grounds for believing an offence has been committed have been removed as compared to the December 2011 version. The category of data at Art.5(e) is very broad and should be better defined to avoid it being used as a general 'miscellaneous' category.

Likewise we welcome the provisions on distinguishing on the basis of the accuracy and reliability of personal data. In both these provisions wording has been added to require this distinguishing 'as far as possible'. We would hope that this is interpreted sensibly as it is not in the interests of

either competent authorities or individuals for personal data to be ambiguous particularly as regards its accuracy or reliability.

Lawfulness of processing (Article 7)

We also welcome the specific circumstances set out to ensure lawfulness of processing, which also cover sensitive data. However, the points previously made relating to a lack of context with sensitive data, and the lack of detail provided in a Directive, could lead to member states simply drafting national law to say that competent authorities can process all sensitive data.

We are also disappointed that the appropriate use of consent has not been recognised. There are circumstances where law enforcement authorities may process personal data in a way that benefits the individual, which is unlikely to be laid down in law and for which consent would be appropriate, such as referring an individual to Victim Support.

Measures based on profiling and automated processing (Article 9)

Obligations on the data controller regarding profiling activity are inconsistent with the same provisions in the Regulation in that profiling to analyse behaviour is no longer included. Analysing behaviour is becoming a more significant aspect of law enforcement activity as technology evolves and carries an increased risk for individuals given the potential consequences for them in this sector.

Chapter III: Rights of the data subject

We are pleased to see consistency with the Regulation relating to the right to rectification, the right to lodge a complaint, the right to a judicial remedy against the national supervisory authority, data controller and data processor, and the right to compensation and liability.

Modalities for exercising the rights of the data subject (Article 10)

Data controllers are required to respond to requests from individuals exercising their rights of access, rectification and erasure 'without undue delay'. It is not clear why the same timeframes required under the Regulation cannot also apply here.

With regard to restrictions on rights, the December 2011 version contained wording in the recitals to stipulate that the controller should assess on a case-by-case basis whether the restriction to the rights should apply, and that any restriction must be in compliance with the Charter of Fundamental Rights of the European Union and with the Convention for the Protection of Human Rights and Freedoms, and in line with the case law of the European Court of Justice and the European Court of Human

Rights, and in particular respect the essence of these rights and freedoms. We recommend reintroducing this wording.

Information to the data subject (Article 11)

The obligations on data controllers are generally consistent with those in the Regulation. However, under the Directive the data controller is not obliged to inform the individual if they intend to transfer personal data to a third country, and it is not clear why this has been excluded, particularly given member states are able to restrict the rights of individuals in certain circumstances.

Related to the point made above on restrictions, and specifically paragraph 5, it is the circumstances, not the data categories, that should be taken into account when applying the exemptions. This point is also valid for similar provisions in Article 13(2) on restricting access rights.

Right to erasure (Article 16)

The December 2011 version required erasure where the processing was not in compliance with the Directive, whereas the final proposal restricts this only to non-compliance with the principles, and provisions on lawfulness of processing and sensitive data. The December 2011 version also provided for restrictions on processing in certain circumstances and this has been changed to simply marking the data. As a result, important safeguards have also been removed relating to the permitted purposes for processing the restricted data, information to individuals and the requirement for time limits for erasure and regular review of retention periods.

Chapter IV: Controller and processor

The obligations on data controllers are consistent with those under the Regulation as regards processors, arrangements with joint controllers, mandating co-operation with the national supervisory authority, and the tasks of the DPO. We also welcome the provision requiring the limited keeping of records.

We are disappointed that various provisions on purpose limitation from the December 2001 version are no longer part of the proposal. The general principle of processing for compatible purposes and safeguards for incompatible purposes should apply to the competent authorities covered by the Directive. The December 2011 version also included provisions on access to data originally processed for other purposes, which is an important aspect of providing safeguards for individuals.

The Directive would also benefit from a provision requiring a receiving authority to respect any use limitations on the personal data imposed by

the sending authority in relation to any disclosures, as provided for in the data protection framework Decision (2008/977/JHA).

Data protection by design and default (Article 19)

As previously stated, we have always promoted privacy by design across all sectors and we welcome its inclusion in the Directive. However, once again the wording is not consistent with the Regulation. One aspect of privacy by design is determining the risks of processing early on in the process and being able to mitigate those risks. Therefore we are extremely disappointed that the provisions requiring DPIAs are no longer part of the proposed Directive. We believe these are particularly important in the field of law enforcement processing of personal data, given the increased risks to individuals of this processing. The removal of this obligation also means that the definition of biometric data serves no purpose, as it was only used in the context of the DPIA provisions.

Documentation (Article 23)

The obligations relating to documentation contain less detail than in the Regulation and it is not clear why competent authorities covered by the Directive should not also need to keep details of at least their DPO and retention periods.

Security of processing (Article 27)

The security obligation provisions do not include guarding against accidental loss or damage, as is provided for under the Regulation. We see no reason for not including this element in the Directive particularly as this aspect is present in both the current Directive (95/46/EC) and the data protection framework Decision (2008/977/JHA).

Notification of a personal data breach to the supervisory authority (Article 28)

Our views on the obligations regarding breach notification have already been covered above in relation to the Regulation. One difference in the Directive is that the national supervisory authority is not able to require the data controller to notify individuals if they consider this is necessary, as is provided for under the Regulation. We do not see why this should be the case given the existence of relevant exceptions and the ability of the controller to appeal against a requirement imposed by the supervisory authority.

Chapter V: Transfer of personal data to third countries or international organisations

We are pleased to see an approach to international transfers in the Directive that reflects the reality of a globalised world, putting the responsibility firmly on the data controller for this aspect of processing, in

the same way as the other aspects of processing. Having said this, we note the two additional derogations relating to safeguarding the legitimate interests of individuals where the law of the member state transferring personal data so provides; and for individual cases for the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties. We would welcome clarification on what circumstances the former aims to cover, and would urge reflection on the latter. Even in individual cases, data controllers should carry out an adequacy assessment that takes account of all the circumstances of the transfer.

International co-operation for the protection of personal data (Article 38)

It is not clear why the Commission needs relations with the supervisory authorities in third countries, and it would seem more appropriate for these relations to be with the EDPB and the national supervisory authorities.

Chapter VI: Independent supervisory authorities

To ensure consistency, it is desirable that member states nominate the same supervisory authority under both the Regulation and Directive.

The Directive is consistent with the Regulation as regards provisions on independence and the EDPB, although this board is given the task of advising the Commission on the adequacy of third countries, whereas this is not listed as a task under the Regulation. It is not clear why this discrepancy exists as this task is equally important for the processing covered by the Regulation.

The powers of national supervisory authorities are harmonised under both instruments, however, the Directive does not include provisions relating to access to premises as is provided for under the Regulation. The ability for the regulator to access the premises of the data controller when necessary should apply to all sectors.

We are pleased to see that under the Directive as under the Regulation supervisory authorities have legally binding powers of intervention, decision and sanction, particularly regarding complaints from individuals, although this wording is contained in recital 56 rather than in the relevant Article.

Chapter VII: Co-operation

Mutual assistance (Article 48)

The Directive provides for mutual assistance between supervisory authorities, however, it does not contain the timescales prescribed in the Regulation. This risks a lack of consistency and the reflection advised

previously relating to the timescales under the Regulation should take account of both instruments. Equally, to ensure consistency across the two instruments, the Directive should include the possibility for supervisory authorities to participate in joint operations.

Chapter VIII: Remedies, liability and sanctions

See the points made above under the Regulation regarding the right to lodge a complaint with a supervisory authority and liability and the right to compensation.

Penalties (Article 55)

We are concerned by the potential lack of harmonisation in relation to penalties. There is a risk of imbalance between the penalties under the Regulation and those under the Directive given that the Directive, unlike the Regulation, does not include any specific provisions for the imposition of administrative sanctions by the supervisory authority.

Chapter IX: Delegated and implementing acts

Please see the points made above under the Regulation regarding delegated and implementing acts.

Chapter X: Final provisions

Relationship with previously concluded international agreements (Article 60)

We welcome the provision requiring international agreements between member states and third countries to be amended in line with the Directive within five years of its entry into force. However, this provision will have less value if the level of data protection in the proposed Directive is not improved.